



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,104	07/29/2003	Jian Huang	CM03751J	6368
22917 MOTOROLA, INC. 1303 EAST ALGONQUIN ROAD IL01/3RD SCHAUMBURG, IL 60196	7590 03/07/2008		EXAMINER GELAGAY, SHEWAYE	
			ART UNIT 2137	PAPER NUMBER
			NOTIFICATION DATE 03/07/2008	DELIVERY MODE ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.Schaumburg@motorola.com  
APT099@motorola.com

### Office Action Summary

**Application No.**

10/629,104

**Applicant(s)**

HUANG ET AL.

**Examiner**

SHEWAYE GELAGAY

**Art Unit**

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 50-58 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 50-58 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-946)
- 3) ☐ Information Disclosure Statement(s) (PTO/CDC)
- 4) ☐ Interview Summary (PTO-413)
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_
- Paper No(s)/Mail Date \_\_\_\_\_

### **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on November 12, 2007. Claims 1-49 has been canceled. New claims 50-58 are added. Claims 50-58 are pending.

### ***Response to Arguments***

2. Applicant's arguments filed 11/12/07 have been considered but are moot in view of the new ground(s) of rejection.

### ***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 50-53 and 55-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zheng et al. (hereinafter Zheng) in view of Law et al. "Key Management with Group-Wise Pre-Deployed Keying and Secret Sharing Pre-Deployed Keying" (hereinafter Law) and in view of Diffie et al. (hereinafter Diffie) U.S. Re.36,946. As per claims 50 and 55:

Zheng teaches a method for secured software patching and upgrade in a distributed wireless sensor network, which comprises:

receiving a software upgrade with a root node; (page 6, paragraphs 88-89)

communicating the software upgrade from the root node to a nodes acting as software upgrade repositories; (page 6, paragraphs 88-89 and 96) and

a patch key being used by the nodes to authenticate a software upgrade .(page 9, paragraph 133; page 11, paragraphs 163-164)

Zheng does not explicitly teach communicating a session key, a patch key length, and a prime modulus to the nodes acting as software upgrade repositories, causing the nodes to generate a patch key with the session key, patch key length, prime modulus, a Diffie-Hellman algorithm, and a locally generated random number. Law in analogous art, however, discloses generating patch keys locally on each node according to the Diffie-Hellman algorithm. (page 2, section 4) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Zheng with Law in order to reduce the secret from being divulged to untrusted nodes by using implementing a system that makes use of shared key without reconstructing the key itself. (page 2, section 4; Law)

Both references do not explicitly disclose communicating a session key and a patch key length. Diffie in analogous art, however, discloses communicating a session key and a patch key length. (col. 4, lines 35-64) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Zheng and Law with Diffie in order to provide secure communication protocol that provides for both privacy of the wireless data communication as well as the authenticity of the communicating parties. (col. 1, lines 43-45; Diffie)

As per claims 51 and 56:

The combination of Zheng, Law and Diffie teaches all the subject matter as discussed above. In addition, Zheng further discloses wherein the patch key length varies on a branch of a spanning-tree. (page 6, paragraphs 88-89 and 96)

As per claims 52-53 and 57-58:

The combination of Zheng, Law and Diffie teaches all the subject matter as discussed above. In addition, Zheng further discloses a method providing at least one root node of the network as a gateway to another network. (page 9, paragraph 140)

3. Claim 54 is rejected under 35 U.S.C. 103(a) as being unpatentable over Zheng et al. (hereinafter Zheng) in view of Law et al. "Key Management with Group-Wise Pre-Deployed Keying and Secret Sharing Pre-Deployed Keying" (hereinafter Law) and in view of Diffie et al. (hereinafter Diffie) U.S. Re.36,946 and in view of Laroia et al. (hereinafter Laroia) US Patent Number 6,961,595.

As per claim 54:

The combination of Zheng, Law and Diffie teaches all the subject matter as discussed above. None of the references explicitly disclose wherein the nodes acting as software upgrade repositories exist on orthogonal branches of the network. Laroia in analogous art, however, teaches wherein the nodes acting as software upgrade repositories exist on orthogonal branches of the network. (col. 4, lines 44-51) Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to modify the method disclosed by Zheng, Law and Diffie with Laroia in order to

avoid interference from transmission signals generated by multiple nodes in the same cell. (col. 4, lines 49-51; Laroia)

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHEWAYE GELAGAY whose telephone number is (571)272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137